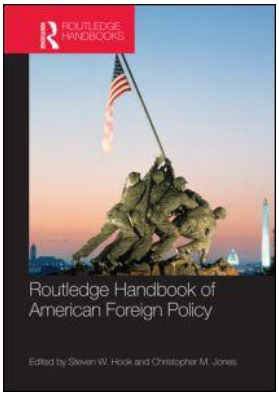

Routledge Handbook of American Foreign Policy

Steven W. Hook, Christopher M. Jones

National Security Intelligence

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9780203878637.ch15
Loch K. Johnson
Published online on: 31 Aug 2011

15

National Security Intelligence

Loch K. Johnson

The subject of national security intelligence—information provided to a nation's leaders by secretive government agencies to protect citizens against threats from domestic or foreign sources—has been around since the days of antiquity. Down through the years all civilizations have had spies working for them and against them. Only in the past three decades, however, has the formal study of national security intelligence reached maturity and a degree of prominence as a subfield of international affairs.

The watershed year was 1975. That year the U.S. government conducted three major inquiries into charges of domestic spying by the Central Intelligence Agency (CIA), the nation's most well-known secret service, referred to as "the Agency" by insiders (Johnson 1986).[1] Professor Harry Howe Ransom of Vanderbilt University observed that before this "Year of Intelligence" the intelligence studies cupboard was, if not bare, then scantily stocked.[2] Then the trio of investigative panels bulldozed into public view a mountain of previous classified information about America's intelligence agencies. These disclosures whet the appetites of researchers and stirred widespread interest in the question of how secret agencies should be supervised in open societies. The decades that followed have seen a stunning proliferation of books (see Johnson 2007) and articles on intelligence, as well as the emergence of credible scholarly journals dedicated to intelligence studies.[3]

The Importance of National Security Intelligence

In addition to the spy inquiries in the United States in 1975, the terrorist attacks carried out by the terrorist organization al Qaeda on September 11, 2001, were another—and brutal—reminder of the importance of national security intelligence. If only the CIA had been able to place an agent high in the al Qaeda organization who could have tipped off U.S. authorities about the planned hijackings. If only the Federal Bureau of Investigation (FBI), the most prominent domestic intelligence agency in the United States, had been more successful at tracking down the terrorists in California earlier in 2001. If only the National Security Agency (NSA), the largest of the American espionage organizations, had translated more quickly from Farsi into English intercepted telephone messages between Qaeda lieutenants that hinted at an approaching attack. If only airport security had been warned about the immediacy of possible hijackings and provided profiles and photographs (which the CIA and the FBI had on

file) of at least some of the terrorists. Mistakes were made by intelligence officers and political leaders alike that might have prevented the aerial terrorism that claimed almost 3,000 lives that horrible day.

Intelligence practitioners speak of "mysteries" and "secrets." Mysteries are subjects that a nation would like to know about in the world, but which are difficult to fathom in light of the limited capacity of human beings to foretell the course of history—say, the question of who might be the next leader of Germany or China, or whether Pakistan will be able to survive the presence inside its borders of Taliban insurgents and al Qaeda terrorists. Secrets are more susceptible to human understanding, although even they may be difficult to unveil, say, the number of nuclear submarines in the Chinese navy, the identity of Russian agents who have infiltrated the North Atlantic Treaty Organization (NATO), or the efficiencies of North Korean rocket fuel.

With the right spy in the right place, with surveillance satellites in the proper orbit, or with reconnaissance aircraft (with or without human pilots) that can penetrate enemy airspace, a nation might be able to uncover secrets. With respect to mysteries, though, national leaders must rely largely on their own judgments and the thoughtful speculation of intelligence analysts to provide the contours of an answer. Either way, prudent nations and other organizations (such as terrorist cells) create intelligence agencies to ferret out secrets and ponder mysteries.

Whatever one's choice of definition for national security intelligence, the critical point is that espionage agencies engage in a several activities in support of the national interest. In the spirit of capturing this diversity of responsibilities, one can say that security intelligence has to do with a cluster of government agencies that conduct secret missions, including covert action, counterintelligence, and, foremost, the collection and analysis of information (from a mixture of covert and open sources) for the purpose of illuminating the security deliberations of policy officials with timely, accurate knowledge of potential threats and opportunities.

Multiple Meanings and Missions

Gathering intelligence is frustrating because mistakes are inevitable. No one has a crystal ball to predict the future. Nonetheless, in this vexing world of uncertainty, ambiguity, fear, and danger, no nation can afford to be without the eyes, ears, and sometimes the hidden fist that secret agencies can provide. National security intelligence, however imperfect, holds out the hope of improving a nation's defenses against foreign and domestic dangers. Though commonly used today, national security intelligence has multiple meanings in the discourse that reflect the functional orientation of practitioners and outside analysts. These meanings are described below.

Intelligence as Secret Information

Observers, and even intelligence specialists and practitioners, do not always agree on the precise meaning of national security intelligence. The major point of disagreement usually pivots around whether a definition ought to be narrow or broad. Defined narrowly (and most commonly), national security intelligence focuses on the primary mission of secret agencies: the gathering and analysis of information that might help to illuminate policy decisions that must be made by national leaders. Refined still further, the definition may focus strictly on the actual product of the collection-and-analysis process: a written report or an oral briefing that conveys a combination of secretly and openly derived information to a government decision maker. The CIA (1991: 13) has defined intelligence simply as the "knowledge and

foreknowledge of the world around us—the prelude to Presidential decision and action." In this instance, national security intelligence means information. Some choose to limit the meaning even more to only secret information—the findings gathered clandestinely by spies, satellites, reconnaissance aircraft, and electronic interceptions, then interpreted by analysts.

Intelligence as a Set of Missions

While intelligence-as-information is the most frequent usage among practitioners, the phrase national security intelligence can refer as well to a number of activities. They include the three primary intelligence missions: collection-and-analysis, covert action, and counterintelligence (examined further below). Here the emphasis is on national security intelligence as a collection of secret activities that a leader might adopt to achieve a foreign policy or security goal.

Intelligence as Process

A third usage focuses specifically on the first and most preeminent of the intelligence missions: collection and analysis. In this case, the phrase points to the process by which information is gathered from the field (perhaps a document stolen by a British agent from a safe in Beijing, or a photograph snapped by a camera on a U.S. surveillance satellite passing over a North Korean vessel in the South China Sea), then transmitted to the offices of decision makers in a nation's seat of government. This upward migration of information collected by secret agencies in the field is often thought of in terms of an "intelligence cycle."

Intelligence as Organization

Finally, national security intelligence may refer to a physical structure, maybe something as rudimentary as a specific tent where analysts are huddled in an encampment bivouacked on a remote battlefield or as elaborate as the CIA's headquarters buildings in Virginia. Whether national security intelligence consists of a top-secret report on Chinese troop deployments in Tibet, a covert action to support a pro-Western African presidential candidate with propaganda radio broadcasts, or the process by which photographs of nuclear reactors in Iran are acquired by a drone (an unmanned aerial vehicle, or UAV), assessed by photo-interpreters, and distributed to decision councils, one must be aware of the complex bureaucratic structures that house strategic intelligence agencies. It is to this subject that we now turn our attention.

Sources of U.S. Intelligence

America's secret agencies have evolved into a cluster of entities known—in a classic misnomer—as the "intelligence community" (IC). In reality, these agencies are more inclined to display the features of rival tribes than a harmonious community. Eight of the agencies are located within the framework of the Department of Defense, seven are in civilian policy departments, and one—the CIA—is an independent agency. The military intelligence agencies include:

- the NSA, the nation's codebreaking, encrypting, and signals intelligence entity, engaged primarily in telephone eavesdropping;

- the National Geospatial-Intelligence Agency (NGA), dedicated chiefly to taking photographs of enemy troops, weapons, and facilities ("imagery intelligence" or "geo-intelligence"), using cameras mounted on spy satellites in space as well as lower-altitude UAVs and other reconnaissance aircraft;
- the National Reconnaissance Office (NRO), which supervises the construction, launching, and management of the nation's spy satellites;
- the Defense Intelligence Agency (DIA), which analyzes military-related subjects; and
- the four separate intelligence units of the Army, Navy, Air Force, and Marines, each focused on the collection-and-analysis of operational intelligence from places overseas where American personnel serve in uniform.

Together, these military agencies account for nearly all of the U.S. intelligence budget (some $75 billion) and employ a vast majority of the nation's espionage personnel (Aspin-Brown Commission 1996: 49). These agencies absorb such a great portion of the annual intelligence funding because of the high costs of the equipment ("platforms") they use for intelligence-gathering— especially surveillance satellites, but also a sophisticated and growing global fleet of UAVs.

Of the eight civilian intelligence agencies, five have been part of the American intelligence community for decades and three are newcomers. In addition to the CIA, examined below, the four established agencies are located in policy departments:

- the FBI, in the Department of Justice and assigned both a counterintelligence and a counterterrorism mission;
- the Office of Intelligence and Analysis, in the Department of Treasury, which includes among its duties the tracking of petrodollars and the hidden funds of terrorist organizations;
- the Bureau of Intelligence and Research (INR) in the Department of State, the smallest of the secret agencies but one of the most highly regarded for its well-crafted and often prescient reports; and
- the Office of Intelligence and Counterintelligence in the Department of Energy, which monitors the worldwide movement of nuclear materials (uranium, plutonium, heavy water, nuclear reactor parts) and maintains security at the nation's weapons laboratories.

The three newcomers, all brought on board after the 9/11 terrorist attacks, include: Coast Guard Intelligence; the Office of Intelligence and Analysis, in the Department of Homeland Security (DHS); and the Office of National Security Intelligence, in the Drug Enforcement Administration (DEA), which is part of the Justice Department. When admitted to the IC in 2001, Coast Guard Intelligence initially stood alone on the community's organizational ("wiring") diagrams. But when the George W. Bush administration created the DHS in 2003, Coast Guard Intelligence became an offshoot of the department because of their common mission to protect the U.S. homeland and its coastline. The DEA, America's lead agency in the global struggle against drug dealers, has been a part of the Justice Department for decades, but became a member of the intelligence community only in 2006.

The eighth civilian agency is the CIA, treated separately because it is the only intelligence agency located outside the government's policy cabinet. During the Cold War, "the Agency" held special cachet in Washington as the only espionage organization formally established by the National Security Act of 1947. Equally important for status and political clout, it became the home office of the director of central intelligence (DCI), the titular leader of all the intelligence agencies in the United States. Since 2005, the community has been led by a director of national intelligence, who is assisted by deputies (DDNIs), a National Counterterrorism

Center (NCTC), and a panel of top-flight analysts who comprise the National Intelligence Council (NIC).

As the names imply, the CIA and the DCI were originally meant to serve as a focal point for the intelligence establishment, playing the role of coordinators for the community's activities and collators of its "all-source" (all agency) reports in an otherwise highly fragmented mélange of espionage organizations. R. James Woolsey, who held the position of DCI during the early years of the Clinton administration, has described the job of America's intelligence chief. "You're kind of Chairman and CEO of the CIA," he said, "and you're kind of Chairman of the Board of the intelligence community."[4] He emphasized, though, that the director does not have the authority to give "rudder orders" to the heads of the various intelligence agencies. Rather, he said, "it's more subtle"—a matter of personal relationships, conversations, and gentle persuasion: the glue of trust and rapport rarely discussed in textbooks but the essence of successful government transactions.

The Intelligence "Cycle"

In myriad ways, the activities of intelligence agencies are important for understanding international affairs. At the heart of decision making in every nation is the reality of policy officials seated around a table in a well-guarded government conference room, as they decide which direction their nation should take. These deliberations are based on information from many sources—a vast flow of ideas and recommendations from personal aides, cabinet members, lobbyists, the media, academics, think-tank experts, friends, and family. A vital component in this "river" of information, to use a metaphor favored by many intelligence directors, are data collected by a nation's secret services.

One cannot fully comprehend the decisions a government makes (or a terrorist organization, for that matter) without an understanding how its secret agencies operate, and without knowing something about the scope and quality of the information these agencies provide. Despite the many sources of information available to leaders, national security intelligence resides at the center of national decision making—largely because agents and spy machines can pry out information from foreign governments that is unavailable to the Library of Congress or some other organization devoid of secret assets abroad.

The phrase "collection and analysis" is used as shorthand to describe a complex process for the gathering, analysis, and dissemination of information to decision makers. A handy way of envisioning this flow is the theoretical construct known as the intelligence cycle. Despite its oversimplification of a complicated process with many interactive stops and starts, the cycle illustrates the major phases in the life of an intelligence report. The first step is known as "planning and direction."

Planning and Direction

The beginning of the intelligence cycle is critical. Unless a potential target is clearly highlighted when officials gather to establish intelligence priorities ("requirements"), the target is unlikely to receive much attention by those who collect information. The world is a large and fractious place, with some 200 nations and a plethora of groups, factions, gangs, cartels, and terrorist groups, some of whom have adversarial relationships with the democratic regimes. As DCI Woolsey noted after the end of the Cold War in 1991, the United States had slain the Soviet dragon, but "we live now in a jungle filled with a bewildering variety of poisonous snakes." At some point the degree of danger posed by foreign adversaries (or domestic subversives)

becomes self-evident, as in the case of the 9/11 attacks. Unfortunately, however, neither government officials nor anyone else are able to predict exactly when and where danger may strike. As former Secretary of State Dean Rusk (who served in the Kennedy and Johnson administrations) observed, "Providence has not provided human beings with the capacity to pierce the fog of the future."[5]

In the United States, the task of determining intelligence priorities is known as a "threat assessment." Experts and policymakers convene periodically to evaluate the perils that confront the nation. In the model developed by Douglas Garthoff (2005: 240), they establish a ladder of priorities from the most dangerous threats (Tiers 1A and 1B) to the least dangerous (Tier 4). Important, too, are calculations about global opportunities. Intelligence is expected to provide a "heads up" regarding both dangers and opportunities. Bias and guess work enter into the picture, along with the limitations caused by the inherent opaqueness of the future. On which tier should one place the Taliban in Afghanistan? Or in Pakistan? What about China? Iran? What about the Russian Federation, less hostile toward the United States than during the Cold War but still able to destroy every American metropolis in the thirty-minute witchfire of a nuclear holocaust?

A key question looms behind these discussions: how much intelligence is enough? The answer depends on the risks a nation is willing to take about the future—how much "information insurance" its leaders desire. Relevant, too, is the extent of a nation's global interests. Asked if the United States collected too much information, DCI William E. Colby (1973–1976) replied: "Not for a big nation. If I were Israel, I'd spend my time on the neighboring Arab armies and I wouldn't give a damn about what happened in China. We are a big power and we've got to worry about all of the world."[6]

Intelligence Collection

The second phase in the intelligence cycle is collection: going after the information that seems important to national security. Every intelligence agency has its own set of methods ("tradecraft"), known colloquially in the United States by the abbreviation "ints," short for intelligence disciplines. Imagery or photographic intelligence becomes "imint," short for imagery intelligence—or, in new terminology, "geoint" (geospatial-intelligence). Without the untrained eye of a professional photointerpreter, the white-and-black squiggles on a satellite photograph can look more like early television than enemy bases. Signals intelligence becomes "sigint," an umbrellas designation for a spate of operations that collect against electronic targets, such as telephone and other communications ("comint"); data emitted by weapons during test flights (telemetry or "telint"); and additional emissions from enemy weapons and radar systems (foreign instrumentation signals or "fisint"). Human intelligence—the use of agents or "assets," as professionals refer to the foreign operatives who comprise their spy rings—becomes "humint."

Within each of the "ints," intelligence professionals fashion ingenious techniques for stealing secrets from adversaries, say, the contents of a laptop computer used by a foreign government scientist in charge of weapons engineering. The methods can range from sophisticated devices that track foreign military maneuvers through telescopic lenses on satellites orbiting deep in space, to the planting of miniature microphones in the breasts of pigeons trained to roost on the window ledges outside foreign embassies. Best of all would be a reliable asset close to a senior official in another country, whether a staff aide or a mistress.

Another prominent int is "osint" or open-source intelligence: information gleaned from non-secretive sources, such as libraries or the foreign media. Is there information in the public domain about whether the desert sands near Tehran are firm enough to support helicopters, or

must an intelligence asset be deployed to find out the answer? This was important matter in 1979, when the Carter administration planned a rescue of U.S. diplomats held in the American embassy in Iran. Today, in the United States, the DNI has a new Center for Open Source Intelligence, which studies what information is missing and will have to be acquired through clandestine means. Since the end of the Cold War, roughly 90 percent—some say as much as 95 percent—of all intelligence reports is comprised of osint, such as information from Iranian blogs on the Internet which can sometimes offer revealing glimpses into that secretive society.

The newest int—measurement and signatures intelligence or "masint," another technical form of intelligence gathering—can be valuable, too. Here the methodology involves testing for the presence of telltale signs of gases, or other chemical and biological indicators, that might reveal the presence of illicit materials, say, waste fumes in a factory that indicate the production of nerve gas. Between 1994 and 2008, for example, the intelligence unit in the U.S. Energy Department reportedly spent some $430 million on nuclear detection equipment at international border crossings, especially along Russia's frontiers (Bronner 2008: A27).

Intelligence professionals make a distinction between humint and technical intelligence collection ("techint")—the latter an acronym that lumps together all of the machine-based means of gathering information. The vast majority of funds spent on collection go into techint. This category includes geoint and sigint satellites; large NSA listening antennae; and reconnaissance aircraft, like the U-2 and A-12 spy planes in the United States, and their successor the SR-21, as well as the popular Predator and Reaper (UAVs fielded over Iraq, Afghanistan, Pakistan, and other nations in the Middle East and South Asia following the 9/11 attacks). Awed by the technological capabilities of spy machines, a nation's leaders choose to spend sizable appropriations on their construction and deployment, prodded by corporations that lobby for funding to build the platforms. This fascination with intelligence hardware has continued into the Age of Terrorism, even though the spy machines are less useful against ghost-like terrorists. Cameras on satellites or airplanes are unable to peer inside the canvas tents, roofed mud huts, or mountain caves in Afghanistan or Pakistan, where al Qaeda and Taliban members meet to plan their deadly operations, or into the deep underground caverns where North Koreans construct atomic bombs. As an intelligence expert (Emerson 1988: 35) notes, often one "needs to know what's inside the building, not what the building looks like."

In contrast to techint spending, the United States devotes only a single-digit percentage of its annual intelligence budget to humint (Millis 1994). The FBI reportedly has more agents in New York City than the CIA has assets around the globe. On occasion, sigint satellites capture revealing information about adversaries, such as telephone conversations between international drug lords; and the photography yielded by geoint satellites on such matters as Chinese missile sites, North Korean troop deployments, Hamas rocket emplacements in Gaza, or the construction of nuclear reactors in Iran are of obvious importance. In the case of terrorism, though, a human agent well situated inside the al Qaeda organization would be worth a dozen billion-dollar satellites.

Humint is no panacea. Within closed societies like North Korea and Iran, indigenous spies are difficult to recruit. Even if successfully recruited, they are often untrustworthy. Neither boy scouts nor nuns, they are known to fabricate reports, sell information to the highest bidder, and scheme as false defectors or double-agents. A recent example is the German agent Rafid Ahmed Alwan, an Iraqi defector prophetically codenamed "Curveball." A former scientist, he persuaded the German intelligence service in 2002 that weapons of mass destruction (WMDs) existed in Iraq. Subsequently, the CIA took the bait through its intelligence liaison relationship with the Germans. Only after the second Persian Gulf War began in Iraq, in 2003, did Curveball's bona fides fall into doubt among German and CIA intelligence officials; he was, it turned out, a consummate liar (CBS News 2007).

Now and then, however, an asset can provide extraordinarily helpful information, as did the Soviet military intelligence officer Oleg Penkosky during the Cold War. In 1962, information from him helped the United States identify the presence of Soviet nuclear missiles in Cuba. Based on occasional successes like Penkosky, the United States and most other countries persevere in their quest for reliable espionage assets. In the aftermath of 9/11 and the WMD errors in Iraq, the Kean and the Silberman-Robb Commissions criticized America's lack of assets in important parts of the world. President George W. Bush authorized a 50 percent increase in the number of CIA operations officers, leading in 2004 to the largest incoming class of clandestine officers in the Agency's history.[7]

The Processing of Intelligence

In the third phase of the intelligence cycle, the information collected must be decoded (if encrypted), translated, and put into a form that the president or the prime minister can readily comprehend. This is known as processing: the conversion of "raw" intelligence, whether photographs or e-mail intercepts, into a readable form.

Intelligence pours into the capitals of the larger nations like a fire hose held to the mouth, to use a metaphor made popular by a former NSA director, Admiral Noel Gayler. Each day, some four million telephone, fax, and e-mail intercepts—often in difficult codes that must be deciphered—flood the NSA. Hundreds of satellite photographs arrive at the NGA. This volume is unlikely to dissipate. Every minute, for instance, a thousand people around the world sign up for a new cell phone. Moreover, nations are always short on translators, photo-interpreters, and code-breaking mathematicians. In response to a query about the major problems facing U.S. intelligence, no wonder Vice Admiral J.M. "Mike" McConnell remarked when he was NSA director: "I have three major problems: processing, processing, and processing."[8]

The day before the 9/11 attacks, the NSA intercepted a telephone message in Farsi from a suspected Qaeda operative. Translated on September 12—too late to help—the message proclaimed: "Tomorrow is zero hour" (Woodward 2004: 215). Whether a more rapid translation might have led to a tightening of U.S. airport security procedures on the morning of September 11 and thwarted the attacks is anyone's guess, but it may have. Today, the vast majority of information gathered by intelligence agencies is never examined; it gathers dust in warehouses—the fate of an estimated 90 percent of what the U.S. intelligence community collects, and as much as 99 percent of the telephone intercepts collected by the NSA.[9] Here is a supreme challenge for the government's information technology (IT) specialists: improving the nation's capacity to sift rapidly through incoming intelligence data, separating the "signals" from the "noise," that is, the wheat from the chaff.

Intelligence Analysis

Analysis, the next phase, lies at the heart of the intelligence cycle: the task of bringing insight to the information that has been collected and processed. The method is straightforward, namely, hiring smart people to pore over all the information from open and secret sources. If the intelligence community is unable to provide reliable interpretations ("assessments," in the British phrase) about what the information means, each of the preceding steps in the cycle is for naught.

Here's the bad news: intelligence analysts will always be taken by surprise from time to time, a fate guaranteed by the twin dilemmas of incomplete information about world affairs

and the uncertain light of the future (Betts 2007). Former Secretary of State Rusk suggested that all intelligence reports ought to start off with the honest caveat, "Damned if I know, but if you want our best guess, well, here it is."[10] Not all the news is bad, though. Western nations have taken long strides toward improving their intelligence capabilities against the enemies of democracy. The $75 billion spent each year by the United States, for example, has allowed officials to deploy the largest and—at least in terms of spy machines—the most sophisticated espionage apparatus ever devised by humankind. This brings in a torrent of information, much of which improves the nation's safety.

Intelligence Dissemination

The final step in the intelligence cycle is to provide decision makers with the information they need to improve their understanding of the world before they make national commitments. This would seem easy enough: just provide the written reports, oral briefings, or secure e-mail messages they require to help their decision making. In fact, though, this step is as difficult as the others—and in some ways it holds the greatest dangers of all.

This stage is difficult because decision makers are fast-moving people who often don't have time to sit still for an intelligence briefing, or even to read an intelligence report. Further, they may reject information that doesn't conform with their preconceived notions; that is, they will "politicize" intelligence by "cherry-picking" the findings and embracing only those items that support their political views, or otherwise twist intelligence reports to suit their own partisan objectives. The greatest danger of all for an intelligence officer is to fall into this trap of politicization, allowing politicians to distort all of their hard efforts throughout the intelligence cycle to obtain solid, reliable information.

Controversies Over Covert Action

In many nations, the importance of intelligence services extends beyond the stream of information and insight they may provide. Intelligence agencies may also engage in covert action—secret operations that are nothing less than an attempt to change the course of history. This mission to "give history a push," as a senior CIA operative has put it, involves the use of propaganda, political and economic operations, and paramilitary activities or warlike endeavors, which can include assassination plots against foreign leaders.[11] These "dirty tricks," as they are characterized by critics, can be attractive to leaders who seek quick and (they hope) quiet measures to gain an advantage over global competitors. Yet sometimes covert action has brought grief and disrepute to its practitioners for violating the canons of propriety and international law, as the CIA's 1961 Bay of Pigs fiasco in Cuba reminds us.

During the Cold War, the main concern of the CIA's Covert Action Staff (the CAS, now known as the Special Activities or SA Division) was, according to one of its chiefs, "the global challenge of communism … to be confronted whenever and wherever it seemed to threaten our interests" (Tovar 1981: 194–195). A Cold War DCI, William Colby (1973–1976), reasoned that covert action was vital to counteract the political and subversive threat posed by Soviet intelligence (KGB) operations in Europe and around the world—just as NATO was critical as a line of military defense and the Marshall Plan a bulwark against Soviet economic encroachments in Western Europe. When threats arise to America's interests in the world, "it is better that we have the ability to help people in these countries where that will happen, quietly and secretly," Colby (1978) advised, "and not wait until we are faced with a military threat that has to be met by armed force."

In a phrase, taking a stand against communism was the raison d'etre for covert action during the Cold War. Whether such targets as Iran (1953), Guatemala (1954), Angola (1975), and Chile (1964–1972) qualified as truly important is a matter of debate. With respect to Angola, a CIA official maintained that "ultimately, the purpose was to throw the Soviets out, at which point we would leave, too." Critics, though, find these arguments unpersuasive. With respect to Nicaragua during the 1980s, the German Nobel laureate in literature, Günter Grass, asked plaintively: "How impoverished must a country be before it is not a threat to the U.S. government?"[12] Senator Frank Church (1976: 8), who led an inquiry into the subject of covert action in 1975, concluded that "our targets were leaders of small, weak countries that could not possibly threaten the United States."

The Implementation of Covert Action

The CIA has been the organization called upon by the president of the United States and his National Security Council (NSC) to conduct covert actions. The agency's infrastructure for this purpose ("the plumbing," in CIA-speak) consists of the National Clandestine Service (NCS); the Special Activities Division and its paramilitary wing, the Special Operations Group (SOG); overseas stations; personnel on loan from the military; and civilian contractors. The role of the president in the approval of a covert action was meant to be tightly concealed, through the practice "plausible deniability." According to this "doctrine," presidents would have to be as pure as Caesar's wife; the reputation of the United States had to be protected if a covert action ran amok and ended up on the front pages of the world's newspapers. Keeping the White House at a distance from unsavory activities would allow a president to claim publicly, "I never authorized this inappropriate operation and I am taking measures to punish those who carried it out."

When the president is kept at arm's length from covert actions, however, they lack the proper accountability that comes with explicit White House approval. In 1961, the Soviet's shot down a CIA U-2 spy plane over their territory on the eve of a Washington-Moscow political summit. President Eisenhower swallowed hard and decided to acknowledge responsibility for the risky surveillance operation. Accountability had trumped plausible denial. In the midst of a spy scandal in the United States during the 1970s, Congress formally buried the old doctrine of deniabilty in favor of legislation that required formal presidential approval of all important covert actions (the Hughes-Ryan Amendment of 1974).

Another serious question arose in the 1980s and continues today about the reliability of covert action accountability. As a result of Pentagon officials and private contractors edging into this domain, critics have called for closer supervision over covert actions (see Kibbe 2007; Prados 2007; and Shorrock 2008). The improper use of organizations other than the CIA to conduct this "third option" (between sending in the Marines and relying on diplomacy) produced a scandal of major proportions during the Reagan administration: the Iran-contra affair. The administration's efforts to support the contras in Nicaragua against the quasi-Marxist Sandinista regime operation took on the dimensions of a scandal for two reasons. First, the covert action was never reported to Congress, as required by the Hughes-Ryan Amendment and the Intelligence Oversight Act of 1980.[13] Further, lawmakers had passed a series of specific laws that prohibited covert action in Nicaragua (the Boland Amendments, named after their chief sponsor, Edward P. Boland [D-Mass.], chairman of the House Permanent Select Committee on Intelligence). When the story of the improper covert actions leaked to a Middle East newspaper and played back into the United States, lawmakers realized that they had been stiffed by administration officials and began a full-scale investigation (see Inouye-Hamilton Committee 1987).

The Methods of Covert Action

Covert action, aimed chiefly at communist regimes during the Cold War and terrorist factions today, may be grouped into four general categories: propaganda, political activities, economic disruptions, and paramilitary (PM) operations. Propaganda schemes might include planting newspaper articles abroad with the help of a "media asset" or secretly leafleting abroad against a cause anathema to a nation's interests. Political activities could entail behind-the-scenes election campaigns against adversaries, or providing money and advertising for friends. Economic disruptions attempt to undermine an adversary by counterfeiting its national currency, blowing up its power plants, mining its harbors, and planting viruses in its computers. An authority (Daughery 2004: 89) refers to this latter form of covert action—secret information warfare—as "the covert action of the future." Paramilitary initiatives can extend from supplying weapons to friends overseas and advising surrogates in secret wars against common adversaries, to the extreme measure of carrying out assassination plots against foreign leaders.

Perhaps the most controversial form of PM covert action has been the use of assassination as a method to eliminate vexing foreign leaders. Fidel Castro attracted the full attention of the CIA's Covert Action Staff and its Special Operations Group during the Kennedy and Johnson administrations. The agency emptied its medicine cabinet of drugs and poisons in various attempts to kill, or at least debilitate, the Cuban leader. In one operation, the CIA placed depilatory powder in Castro's shoes when he traveled abroad, which would presumably enter his bloodstream through his feet and cause his famous charismatic beard to fall off his chin. It also impregnated his cigars with LSD and deadly botulinum toxin; dusted his underwater diving suit with Madura foot fungus; tried to find someone in Cuba close enough to Castro to inject the highly poisonous substance Blackleaf-40 into his skin, using a needle-tipped ballpoint pen; and sneaked an attractive woman into his kitchen to place a poison in his soup.

All of these efforts failed, for Castro was elusive and well protected by an elite security guard trained by the KGB. So the agency raised the stakes, turning to the Mafia for assistance: Chicago gangster Sam Giancana; Cosa Nostra chief for Cuba Santo Trafficante; mobster John Rosselli. They still had contacts in Cuba from pre-Castro days when Havana was a world gambling mecca. No doubt assuming that the U.S. government would back off Mafia prosecutions in return for some help against Castro, they volunteered to assemble and infiltrate assassination teams of Cuban exiles and other assassins into Cuba. These efforts failed as well.

The Vital Role of Counterintelligence

Every nation's intelligence agencies have another important mission known as counterintelligence. Here the purpose is to guard a nation's secrets and institutions against penetration and deception by a hostile foreign government or faction. In the United States, an Executive Order offers this definition of counterintelligence (CI):

> Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, other intelligence activities, sabotage or assassination conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.[14]

A former Soviet practitioner of the art form has stated the objective more simply as activities performed by "security organizations authorized and directed by the government to protect the State and its citizens against espionage, sabotage and terrorism."[15] Simpler still, one can

say that the task of CI is to thwart hostile acts perpetrated against one's nation by foreign intelligence agencies, terrorist factions, and internal subversives. Foreign adversaries will attempt to burrow into a rival (and sometimes a friendly) government, mole-like, in search of secrets and to sow disinformation. The Soviets succeeded in penetrating the CIA and the FBI at high levels during the waning years of the Cold War, as well as the British, German, and French intelligence services—with disastrous effects for the West.

In the United States, the counterintelligence threat has shifted somewhat in recent years. Between 1945 and early 2008, about 45 percent of the 247 foreign agents arrested in the United States were engaged in espionage for the Soviet Union or Russia; in contrast, of the 37 arrested since 2000, 65 percent were spying either for China or for countries in the Middle East (Sims and Gerber 2009: 3). Experts make a distinction between counterintelligence and counterterrorism. Both have the same goals outline in the definitions above, but counterterrorism focuses on a specific threatening target: non-state organizations, like Al Qaeda.

Every nation seeks to thwart the presence of foreign spies in its midst and is willing to expend large amounts of resources on counterintelligence to defend against this danger. The end result is a game of cat and mouse played by spy catchers inside the inner sanctums of national capitals around the world.

An Intelligence Studies Agenda

As we have seen, national security intelligence in the United States comes from many sources and takes many forms. This realm of foreign policy is routinely criticized for its failure to prevent such catastrophic events as the September 2001 terrorist attacks. Further, critics charge that intelligence agencies, which by their nature are highly secretive, are not held responsible for their policies and actions. In democratic regimes, the matter of intelligence accountability is vital to those who fear the rise of a Gestapo within their own society. In the United States, former DCI Robert M. Gates (1996: 559) stated the case for intelligence accountability: "some awfully crazy schemes might well have been approved had everyone present [in the White House] not known and expected hard questions, debate, and criticism from the Hill." And when, on a few occasions, Congress was left in the dark, and such schemes did proceed, it was nearly always to the lasting regret of the presidents involved.

Regardless of these compelling reasons for intelligence accountability, most observers agree that members of Congress and parliamentarians in other democracies are performing far below their potential when it comes to the supervision of their nation's secret agencies. Former Senator Gary Hart (1993: 144) has emphasized that, regardless of the policy domain, "public interest and insistence is necessary for reform." Intelligence oversight is a neglected stepchild even within the democracies—and will remain so, unless citizens demand otherwise.

Here, then, are the elements of what is meant by "national security intelligence." It is a vast and complicated topic, with both technical and humanistic dimensions—all made doubly hard to study and understand because of the thick veils of secrecy that surround a nation's security apparatus. Fortunately, from the point of view of democratic openness as well as the canons of scholarly inquiry, many of these veils have fallen in the past three decades as a result of government inquiries into intelligence failures and wrongdoing, accompanied by a more determined effort by researchers to probe the hidden side of government. The research by a wide range of scholars cited in this chapter is a testament to the insights about national security that can accrue from a steady probing of intelligence organizations and their activities.

Much remains to be done and national security imperatives, quite properly, will never permit full transparency in this sensitive domain. In a democracy, however, the people must

have at least a basic understanding of all their government agencies, even the shadowy world of intelligence. The Cold War was essentially a struggle between Western and communist spy organizations, demonstrating the importance of intelligence. Sometimes these secret agencies have been the source of great embarrassment to the government, as with the Bay of Pigs fiasco, the CIA assassination attempts during the Eisenhower and Kennedy administrations, the domestic spy scandals of the mid-1970s, and the Iran-*contra* scandal a decade later. Intelligence errors can have enormous consequences, too, as when the United States invaded Iraq in 2003 based in part on a faulty intelligence assessment that Saddam Hussein, the Iraqi dictator, was developing weapons of mass destruction that could soon strike the United States and the United Kingdom. Further, intelligence organizations and operations are costly. For all of these reasons, intelligence deserves the public's attention and continuing scrutiny by the scholarly community.

Notes

1 The investigations included the Pike Committee in the U.S. House of Representatives (led by Otis Pike [D-New York]), the Rockefeller Commission appointed by the Ford White House (led by Vice President Nelson Rockefeller), and the Church Committee in the U.S. Senate (led by Frank Church [D-Idaho]). The latter was the most thorough and its influence has been the most enduring. For its findings, see U.S. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, "Foreign and Military Intelligence," *Final Report*, S. Rept. 94-755, vol. 1, 94th Cong., 2d. Sess. (Washington, D.C.: U.S. Government Printing Office, May 1976).

2 Remark to the author, Washington, D.C. (December 20, 1975).

3 The top journals are *Intelligence and National Security*, *International Journal of Intelligence and Counterintelligence*, and *Studies in Intelligence*.

4 R. James Woolsey, author's interview, CIA Headquarters, Langley, VA (September 29, 1993).

5 Dean Rusk, remark to the author, Athens, Georgia (February 21, 1988).

6 William E. Colby, remark to the author, Washington, D.C. (January 22, 1991).

7 See, respectively, The Kean Commission's 9/11 Commission Report, *Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton, 2004), p. 415; the Silberman-Robb Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Final Report* (Washington, D.C.: U.S. Government Printing Office, 2005), pp. 410–411; and George Tenet, with Bill Harlow, *At the Center of the Storm: My Years at the CIA* (New York: HarperCollins, 2007), p. 24.

8 Author's interview with a senior NSA official who quoted the NSA Director, Washington, D.C. (July 14, 1994).

9 John L. Millis, speech, Central Intelligence Retirees Association, Arlington, VA (October 5, 1998), p. 6.

10 Dean Rusk, remark to the author, Athens, Georgia (February 21, 1988).

11 Author's interview with a senior CIA official in the Operations Directorate, Washington, D.C. (February 1986).

12 Quoted in *The Nation* (March 12, 1983), p. 301.

13 Section 662(a) of the Foreign Assistance Act of 1974; Section 662 of the Foreign Assistance Act of 1961 (22 U.S.C. 2422).

14 Executive Order 12333, Sec. 3.5, as amended on July 31, 2008.

15 Colonel General Oleg Danilovich Kalugin, former head of the KGB First Chief Directorate, cited by Paul J. Redmond, Jr., "The Challenges of Counterintelligence," in Loch K. Johnson, ed., *The Oxford Handbook of National Security Intelligence* (New York: Oxford University Press, 2010), pp. 537–554, quote at p. 537.

References

Aspin-Brown Commission. 1996. *Preparing for the 21 Century: An Appraisal of U.S. Intelligence*. Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, March 1. Washington, D.C.: U.S. Government Printing Office.

Betts, Richard K. 2007. *Enemies of Intelligence: Knowledge & Power in American National Security*. New York: Columbia University Press.

Bronner, Michael. 2008. "When the War Ends, Start to Worry," *New York Times*, August 16, A27.

CBS News. 2007. "Faulty Intel Source 'Curve Ball' Revealed," *60 Minutes*, November 4, http://www.cbsnews.com/stories/2007/11/01/60minutes/main3440577.shtml.

Central Intelligence Agency. 1991. *Fact Book on Intelligence*. Langley, VA: Office of Public Affairs, Central Intelligence Agency.

Church, Frank. 1976. "Covert Action: Swampland of American Foreign Policy," *Bulletin of the Atomic Scientists* 32 (February): 7–11.

Colby, William E. 1978. "Gesprach mit William E. Colby" [Conversation with William E. Colby]. *Der Spiegel* 4 (January 23), author's translation.

Daughery, William J. 2004. *Executive Secrets: Covert Action & the Presidency*. Lexington: University Press of Kentucky.

Emerson, Steven. 1988. *Secret Warriors: Inside the Covet Military Operations of the Reagan Era*. New York: Putnam.

Garthoff, Douglas F. 2005. *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005*. Washington, D.C.: Center for the Study of Intelligence.

Gates, Robert M. 1996. *From the Shadows*. New York: Simon and Schuster.

Hart, Gary. 1993. *The Good Fight: The Education of an American Reformer*. New York: Random House.

Inouye-Hamilton Committee. 1987. *Hearings and Final Report*. Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition, U.S. Senate, and House Select Committee to Investigate Covert Arms Transactions with Iran. Washington, D.C.: U.S. Government Printing Office.

Johnson, Loch K. 1986. *A Season of Inquiry*. Lexington, KY: University Press of Kentucky.

———. 2007. "An Introduction to the Intelligence Studies Literature." In *Strategic Intelligence, Vol. I: Understanding the Hidden Side of Government*, Loch K. Johnson, ed., 1–20. Westport, Conn.: Praeger.

Kibbe, Jennifer. 2007. "Covert Action and the Pentagon." In *Strategic Intelligence: Covert Action,* Loch K. Johnson, ed., 145–156. Vol. 3. Westport, Conn.: Praeger.

Millis, John L. 1994. "Our Spying Success Is No Secret." Letter to the editor, *New York Times*, October 12, A27.

Prados, John. 2007. "The Future of Covert Action." In *Handbook of Intelligence Studies*, Loch K. Johnson, ed., 289–298. New York: Routledge.

Shorrock, Tim. 2008. *Spies for Hire: The Secret World of Intelligence Outsourcing*. New York: Simon and Schuster.

Sims, Jennifer E., and Burton Gerber, eds. 2009. *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence*. Washington, D.C.: Georgetown University Press.

Tovar, B. Hugh. 1981. "Strengths and Weaknesses in Past U.S. Covert Action." In *Intelligence Requirements for the 1980s: Covert Action*, Roy Godson, ed., 194–195. Washington, D.C.: National Strategy Information Center.

Woodward, Bob. 2004. *Plan of Attack*. New York: Simon and Schuster.